

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-244584

(43)Date of publication of application : 19.09.1995

(51)Int.Cl.

G06F 9/06
G06F 12/14

(21)Application number : 06-032601

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 02.03.1994

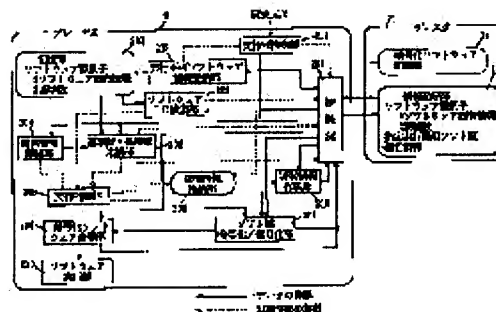
(72)Inventor : OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
MIYAJI MITSUKO

(54) SOFTWARE PROTECTION SYSTEM

(57)Abstract:

PURPOSE: To attain execution by an optional execution device by a procedure for changing a specified execution device in a software protection system which can not be executed by an execution device other than the specified one.

CONSTITUTION: Whether a software identifier(ID) recorded in an information recording part 12 of a disk 1 is stored in a storage part 203 or not is retrieved. When the corresponding ID is stored in the storage part 203, the accumulated number of IDs is compared with a reference number stored in the storage part 203, and only when the accumulated number is larger, the execution of the software is permitted. Also when the corresponding ID is not stored in the storage part 203, the execution of the software is permitted. In this case, a software key in the recording part 12 is decoded by a software key ciphering/ decoding part 207, ciphered software recorded in a ciphered software recording part 11 is decoded by using the software key and executed by a software execution part 210. At the time of changing a specified execution device, the accumulated number of IDs and the reference value are changed and a software key is rewritten to a key for a changed execution device.



LEGAL STATUS

[Date of request for examination] 14.07.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3344810

[Date of registration] 30.08.2002

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(2)

特開平 7-244584

1

2

【特許請求の範囲】

【請求項 1】 記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、前記記録媒体には、ソフトウェアと、前記ソフトウェアまたは前記記録媒体に固有の第 1 の固有情報と、前記ソフトウェアを実行させるべき実行器に固有の第 2 の固有情報とが格納されており、前記実行器は、前記記録媒体から前記ソフトウェアおよび前記第 2 の固有情報を読み出し、当該第 2 の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるチェック手段、前記ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、前記記録媒体に格納された第 2 の固有情報を、前記実行器指定手段で指定された他の実行器に固有の情報に変換する変換手段、実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、前記実行器指定手段によって実行器の変更先が指定されたとき、前記記録媒体に格納された第 1 の固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けずに前記チェック手段を制御する第 1 の実行制御手段を備える、ソフトウェア保護システム。

【請求項 2】 前記記録媒体には、さらに、前記第 1 の固有情報と対して累積数が格納されており、前記実行不可情報記憶手段には、さらに、前記第 1 の固有情報と対して基準数が記憶されており、前記累積数および前記基準数は、初期値が同一値に選ばれており、前記実行器は、前記実行器指定手段によって実行器の変更先が指定されたとき、前記累積数および前記基準数のそれぞれに所定値を加算する加算手段をさらに備え、前記第 1 の実行制御手段は、前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されていない場合、または前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されているが前記累積数が前記基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行許可を前記チェック手段に与え、前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されてお

り、かつ前記累積数が前記基準数と等しいかまたはそれよりも小さい場合は、当該記録媒体に格納されているソフトウェアの実行不許可を前記チェック手段に与えることを特徴とする、請求項 1 に記載のソフトウェア保護システム。

【請求項 3】 前記記録媒体には、さらに、前記第 1 の固有情報と対して乱数が格納されており、前記実行不可情報記憶手段には、さらに、前記第 1 の固有情報と対して乱数が記憶されており、

10 前記実行器は、さらに前記実行器指定手段によって実行器の変更先が指定されたとき、乱数を発生する乱数発生手段、前記乱数発生手段によって乱数が発生される毎に、当該乱数を前記実行不可情報記憶手段に追加して書き込む乱数書き込み手段、および前記乱数発生手段によって乱数が発生される毎に、前記記録媒体に格納された乱数を書き換える乱数書き換え手段を備え、前記第 1 の実行制御手段は、前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されていない場合、または前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されているが前記記録媒体に格納されている乱数と同一の乱数が前記実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行許可を前記チェック手段に与え、前記記録媒体に格納されている第 1 の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されており、かつ前記記録媒体に格納されている乱数と同一の乱数が前記実行不可情報記憶手段に記憶されている場合は、当該記録媒体に格納されているソフトウェアの実行不許可を前記チェック手段に与えることを特徴とする、請求項 1 に記載のソフトウェア保護システム。

【請求項 4】 前記記録媒体に格納されたソフトウェアは、暗号化されており、前記記録媒体に格納された第 2 の固有情報は、暗号化されたソフト鍵であり、前記チェック手段は、実行器毎に異なる秘密情報を記憶する秘密情報記憶手段と、前記記録媒体から前記ソフト鍵を読み出し、前記秘密情報を用いて復号化するソフト鍵復号化手段と、前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化されたソフト鍵を用いて復号化するソフトウェア復号化手段と、前記復号化されたソフトウェアを実行するソフトウェア実行手段とを含み、前記変換手段は、前記復号化されたソフト鍵を、前記実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能な

50

(3)

特開平7-244584

3

ように暗号化するソフト鍵暗号化手段と、
前記記録媒体に格納された暗号化されたソフト鍵を、前記ソフト鍵暗号化手段によって暗号化されたソフト鍵に書き換えるソフト鍵書き換え手段とを含む、請求項1～3のいずれかに記載のソフトウェア保護システム。

【請求項5】 前記記録媒体には、さらに、前記暗号化されたソフトウェア、前記第1の固有情報、前記暗号化されたソフト鍵および前記累積数の内、少なくともいずれか1つを対象として作成されたデジタル署名情報が格納されており、

前記実行器は、さらに前記記録媒体に格納されているデジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記チェック手段を制御する第2の実行制御手段、

前記実行器指定手段によって実行器の変更先が指定されたとき、前記秘密情報を用いて、前記デジタル署名情報を作成するデジタル署名情報作成手段、および前記記録媒体に格納されたデジタル署名情報を、前記デジタル署名情報作成手段によって作成されたデジタル署名情報に書き換える署名情報書き換え手段を備える、請求項4に記載のソフトウェア保護システム。

【請求項6】 前記記録媒体には、さらに、コピー可能回数が格納されており、

前記実行器は、さらに前記記録媒体をコピーした回数を示す累計数を記憶する累計数記憶手段、

前記記録媒体に格納されたコピー可能回数が前記累計数記憶手段に記憶された累計数よりも大きい場合のみ、当該記録媒体のコピーを実行するコピー制御手段、および前記コピー制御手段が前記記録媒体のコピーを実行する毎に、前記累計数記憶手段に記憶された累計数を更新する累計数更新手段を備える、請求項1～5のいずれかに記載のソフトウェア保護システム。

【請求項7】 ソフトウェアが格納された記録媒体を貸与する場合、貸し主側の実行器で変更手続きを行うことにより、当該ソフトウェアの実行が可能な借り主側の実行器を特定するようなソフトウェア保護システムであって、

前記記録媒体には、

暗号化されたソフトウェアと、

前記ソフトウェアまたは前記記録媒体に固有のソフトウェア／記録媒体固有情報と、

前記貸し主側の実行器に固有の暗号化された第1のソフト鍵と、

前記借り主側の実行器に固有の暗号化された第2のソフト鍵とが格納されており、

前記貸し主側の実行器は、

当該貸し主側の実行器に固有の第1の秘密情報を記憶する第1の秘密情報記憶手段、

前記記録媒体から前記第1のソフト鍵を読み出し、前記

4

第1の秘密情報を用いて復号化する第1のソフト鍵復号化手段、

前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化された第1のソフト鍵を用いて復号化する第1のソフトウェア復号化手段、

前記復号化されたソフトウェアを実行する第1のソフトウェア実行手段、

前記ソフトウェアを実行する前記借り主側の実行器を指定する実行器指定手段、

10 前記復号化された第1のソフト鍵を、前記実行器指定手段で指定された借り主側の実行器でのみ復号可能な第2のソフト鍵に暗号化するソフト鍵暗号化手段、および前記記録媒体に格納された暗号化された第2のソフト鍵を、前記ソフト鍵暗号化手段によって暗号化された第2のソフト鍵に書き換えるソフト鍵書き換え手段を備え、前記借り主側の実行器は、

当該借り主側の実行器に固有の第2の秘密情報を記憶する第2の秘密情報記憶手段、

20 前記記録媒体から前記第2のソフト鍵を読み出し、前記第2の秘密情報を用いて復号化する第2のソフト鍵復号化手段、

前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化された第2のソフト鍵を用いて復号化する第2のソフトウェア復号化手段、

前記復号化されたソフトウェアを実行する第2のソフトウェア実行手段、

前記記録媒体の返却手続きを指示する返却手続き指示手段、

30 実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、

前記返却手続き指示手段によって返却手続きが指示されたとき、前記記録媒体に格納されたソフトウェア／記録媒体固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記第2のソフトウェア実行手段を制御する実行制御手段を備える、ソフトウェア保護システム。

40

【請求項8】 記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、

前記記録媒体には、

暗号化されたソフトウェアと、

前記ソフトウェアまたは前記記録媒体に固有のソフトウェア／記録媒体固有情報とが格納されており、

前記実行器は、

実行器毎に異なる秘密情報を記憶する秘密情報記憶手段、

50

(4)

特開平7-244584

5

前記録媒体から暗号化されたソフトウェアを読み出し、前記秘密情報を用いて復号化するソフトウェア復号化手段、
前記復号化されたソフトウェアを実行するソフトウェア実行手段、
前記ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、
前記復号化されたソフトウェアを、前記実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフトウェア暗号化手段、
前記録媒体に格納された暗号化されたソフトウェアを、前記ソフトウェア暗号化手段によって暗号化されたソフトウェアに書き換えるソフトウェア書き換え手段、
実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、
前記実行器指定手段によって実行器の変更先が指定されたとき、前記録媒体に格納されたソフトウェア／記録媒体固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けずに前記ソフトウェア実行手段を制御する実行制御手段を備える、ソフトウェア保護システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はソフトウェア保護システムに関し、より特定的には、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムに関する。

【0002】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトウェアを始めとする多くの有償マルチメディアソフトウェアが販売されている。ところが、そのソフトウェアの保護は不完全であり、不正にコピーされたソフトウェアが数多く出回っているのが現状である。このような不正なコピーを防ぐために特許法や著作権法等の法律の規制があるが、同時にメカニズム面からのソフトウェア保護も必要である。

【0003】例えば、ソフトウェアを格納する記録媒体（フロッピーディスク等）のフォーマットを特殊なものにすることによって、OS（オペレーティング・システム）で提供されているコピー機能では複製ができないようにする方法がある。しかしながら、このような方法でもビットごとにコピーを行なうタイプのコピーツールを用いれば、多くの場合複製が可能である。また、正規のユーザにとっては、バックアップディスクが作れないといった不都合も生じる。

【0004】また、ソフトウェアを暗号化してコピー防

6

止を行なう方法が提案されている。この方法は、例えば特開昭61-145642号公報に示されている。図7にその構成を示す。図7において、パーソナルコンピュータ501は、暗号機構502を含む。ソフトウェア販売業者によって販売されるプログラム503は、一意的なファイルキーKFで暗号化されており、1つのプログラムファイルとしてディスク（特開昭61-145642号公報では、ディスクと称している）上に書き込まれている。

10 【0005】暗号化されたプログラム503が格納されたディスクを購入するユーザーは、まずソフトウェア販売業者からキー配送センタ504で生成される秘密のパスワードを取得しなければならない。このパスワードにより、暗号化されたプログラム503は、適切に初期設定された暗号機構502を有する予め指定されたパーソナルコンピュータ501だけで解読し実行することができる。この秘密のパスワードは、特定のプログラムおよびこれが復元され実行される特定のコンピュータに対して一意的なものである。このパスワードによれば、他の
20 暗号化されたプログラムをそのコンピュータで復元することはできず、同じ暗号化されたプログラムを他のコンピュータで復元することもできない。また、暗号化されたプログラムが格納されたディスクをコピーしても、予め指定されたパーソナルコンピュータ以外のコンピュータでは復元することはできず、コピーしても意味がなくなる。これによりコピー防止機能が実現されている。

【0006】

【発明が解決しようとする課題】しかしながら、上記従来のソフトウェア保護方式では、正当なソフトウェアの持ち主であっても、ソフトウェアを予め指定された実行器以外では実行できないため、ソフトウェアを他の場所で実行することや、他のユーザにソフトウェアを譲渡することが困難である。

【0007】他の場所での実行を可能にするためには、ソフトウェアを格納した記録媒体だけでなく、予め指定されたパーソナルコンピュータ501も移動することが考えられるが、パーソナルコンピュータ501が一般には記録媒体に比べて大型で移動しにくいことを考慮すると非現実的である。

40 【0008】一方、ソフトウェアの譲渡を有効にするためには、パーソナルコンピュータ501ごとソフトウェアを他のユーザに譲渡することが考えられるが、これもパーソナルコンピュータ501がもともとそのユーザに所属するものであり、複数のソフトウェアを実行するものであることを考慮すると、1つのソフトウェアを他のユーザに譲渡するために本体ごと譲渡するというのもまた非現実的である。この場合、ユーザ側で譲渡先のユーザ用のソフトウェアを作成することも考えられるが、元のソフトウェアが譲渡元でも実行可能であるため、実質的な譲渡が成立しない。

50

(5)

特開平7-244584

7

8

【0009】それゆえに、本発明の目的は、ソフトウェアを他の実行器でも実行でき、かつ不法なコピーも防止し得るソフトウェア保護システムを提供することである。本発明の他の目的は、ソフトウェアを貸与する場合に好適するソフトウェア保護システムを提供することである。本発明のさらに他の目的は、ソフトウェアのコピー回数を制御できるソフトウェア保護システムを提供することである。

【0010】

【課題を解決するための手段】請求項1に係る発明は、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、記録媒体には、ソフトウェアと、ソフトウェアまたは記録媒体に固有の第1の固有情報と、ソフトウェアを実行させるべき実行器に固有の第2の固有情報とが格納されており、実行器は、記録媒体からソフトウェアおよび第2の固有情報を読み出し、当該第2の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるチェック手段、ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、記録媒体に格納された第2の固有情報を、実行器指定手段で指定された他の実行器に固有の情報に変換する変換手段、実行可能なソフトウェアに関する情報を記憶する実行不可情報記憶手段、実行器指定手段によって実行器の変更先が指定されたとき、記録媒体に格納された第1の固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けずにチェック手段を制御する第1の実行制御手段を備えている。

【0011】請求項2に係る発明は、請求項1の発明において、記録媒体には、さらに、第1の固有情報と対にして累積数が格納されており、実行不可情報記憶手段には、さらに、第1の固有情報と対にして基準数が記憶されており、累積数および基準数は、初期値が同一値に選ばれており、実行器は、実行器指定手段によって実行器の変更先が指定されたとき、累積数および基準数のそれぞれに所定値を加算する加算手段をさらに備え、第1の実行制御手段は、記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されているが累積数が基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行許可をチェック手段に与え、記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されており、かつ累積数が基準数と等しいかまたはそれよりも小さい場合は、当該記録媒体に格納されているソフトウェアの実行不許可をチェック手段に与えるこ

とを特徴とする。

【0012】請求項3に係る発明は、請求項1の発明において、記録媒体には、さらに、第1の固有情報と対にして乱数が格納されており、実行不可情報記憶手段には、さらに、第1の固有情報と対にして乱数が記憶されており、実行器は、さらに実行器指定手段によって実行器の変更先が指定されたとき、乱数を発生する乱数発生手段、乱数発生手段によって乱数が発生される毎に、当該乱数を実行不可情報記憶手段に追加して書き込む乱数書き込み手段、および乱数発生手段によって乱数が発生される毎に、記録媒体に格納された乱数を書き換える乱数書き換え手段を備え、第1の実行制御手段は、記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されていない場合、または記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されているが記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行許可をチェック手段に与え、記録媒体に格納されている第1の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されており、かつ記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されている場合は、当該記録媒体に格納されているソフトウェアの実行不許可をチェック手段に与えることを特徴とする。

【0013】請求項4の発明は、請求項1～3のいずれかの発明において、記録媒体に格納されたソフトウェアは、暗号化されており、記録媒体に格納された第2の固有情報は、暗号化されたソフト鍵であり、チェック手段は、実行器毎に異なる秘密情報を記憶する秘密情報記憶手段と、記録媒体からソフト鍵を読み出し、秘密情報を用いて復号化するソフト鍵復号化手段と、記録媒体から暗号化されたソフトウェアを読み出し、復号化されたソフト鍵を用いて復号化するソフトウェア復号化手段と、復号化されたソフトウェアを実行するソフトウェア実行手段とを含み、変換手段は、復号化されたソフト鍵を、実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフト鍵暗号化手段と、記録媒体に格納された暗号化されたソフト鍵を、ソフト鍵暗号化手段によって暗号化されたソフト鍵に書き換えるソフト鍵書き換え手段とを含むことを特徴とする。

【0014】請求項5に係る発明は、請求項4の発明において、記録媒体には、さらに、暗号化されたソフトウェア、第1の固有情報、暗号化されたソフト鍵および累積数の内、少なくともいずれか1つを対象として作成されたデジタル署名情報が格納されており、実行器は、さらに記録媒体に格納されているデジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けずに

50

(6)

特開平7-244584

9

10

うにチェック手段を制御する第2の実行制御手段、実行器指定手段によって実行器の変更先が指定されたとき、秘密情報を用いて、デジタル署名情報を作成するデジタル署名情報作成手段、および記録媒体に格納されたデジタル署名情報を、デジタル署名情報作成手段によって作成されたデジタル署名情報に書き換える署名情報書き換え手段を備えている。

【0015】請求項6に係る発明は、請求項1～5のいずれかの発明において、記録媒体には、さらに、コピー可能回数が格納されており、実行器は、さらに記録媒体をコピーした回数を示す累計数を記憶する累計数記憶手段、記録媒体に格納されたコピー可能回数が累計数記憶手段に記憶された累計数よりも大きい場合のみ、当該記録媒体のコピーを実行するコピー制御手段、およびコピー制御手段が記録媒体のコピーを実行する毎に、累計数記憶手段に記憶された累計数を更新する累計数更新手段を備えている。

【0016】請求項7に係る発明は、ソフトウェアが格納された記録媒体を貸与する場合、貸し主側の実行器で変更手続きを行うことにより、当該ソフトウェアの実行が可能な借り主側の実行器を特定するようなソフトウェア保護システムであって、記録媒体には、暗号化されたソフトウェアと、ソフトウェアまたは記録媒体に固有のソフトウェア／記録媒体固有情報と、貸し主側の実行器に固有の暗号化された第1のソフト鍵と、借り主側の実行器に固有の暗号化された第2のソフト鍵とが格納されており、貸し主側の実行器は、当該貸し主側の実行器に固有の第1の秘密情報を記憶する第1の秘密情報記憶手段、記録媒体から第1のソフト鍵を読み出し、第1の秘密情報を用いて復号化する第1のソフト鍵復号化手段、記録媒体から暗号化されたソフトウェアを読み出し、復号化された第1のソフト鍵を用いて復号化する第1のソフトウェア復号化手段、復号化されたソフトウェアを実行する第1のソフトウェア実行手段、ソフトウェアを実行する借り主側の実行器を指定する実行器指定手段、復号化された第1のソフト鍵を、実行器指定手段で指定された借り主側の実行器でのみ復号可能な第2のソフト鍵に暗号化するソフト鍵暗号化手段、および記録媒体に格納された暗号化された第2のソフト鍵を、ソフト鍵暗号化手段によって暗号化された第2のソフト鍵に書き換えるソフト鍵書き換え手段を備え、借り主側の実行器は、当該借り主側の実行器に固有の第2の秘密情報を記憶する第2の秘密情報記憶手段、記録媒体から第2のソフト鍵を読み出し、第2の秘密情報を用いて復号化する第2のソフト鍵復号化手段、記録媒体から暗号化されたソフトウェアを読み出し、復号化された第2のソフト鍵を用いて復号化する第2のソフトウェア復号化手段、復号化されたソフトウェアを実行する第2のソフトウェア実行手段、記録媒体の返却手続きを指示する返却手続き指示手段、実行不可なソフトウェアに関する情報を記憶する

実行不可情報記憶手段、返却手続き指示手段によって返却手続きが指示されたとき、記録媒体に格納されたソフトウェア／記録媒体固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けずに第2のソフトウェア実行手段を制御する実行制御手段を備えている。

【0017】請求項8に係る発明は、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、記録媒体には、暗号化されたソフトウェアと、ソフトウェアまたは記録媒体に固有のソフトウェア／記録媒体固有情報とが格納されており、実行器は、実行器毎に異なる秘密情報を記憶する秘密情報記憶手段、記録媒体から暗号化されたソフトウェアを読み出し、秘密情報を用いて復号化するソフトウェア復号化手段、復号化されたソフトウェアを実行するソフトウェア実行手段、ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、復号化されたソフトウェアを、実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフトウェア暗号化手段、記録媒体に格納された暗号化されたソフトウェアを、ソフトウェア暗号化手段によって暗号化されたソフトウェアに書き換えるソフトウェア書き換え手段、実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、実行器指定手段によって実行器の変更先が指定されたとき、記録媒体に格納されたソフトウェア／記録媒体固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けずにソフトウェア実行手段を制御する実行制御手段を備えている。

【0018】

【作用】請求項1に係る発明においては、ソフトウェアを実行させるべき実行器に固有の第2の固有情報を記録媒体に格納しておき、実行器では、記録媒体からソフトウェアおよび第2の固有情報を読み出し、当該第2の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるようにしている。これによって、ソフトウェアを実行可能な実行器を予め特定することができる。また、ソフトウェアを実行する実行器の変更先が指定されると、記録媒体に格納された第2の固有情報を、指定された他の実行器に固有の情報に変換するようにしている。これによって、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。

(7)

特開平7-244584

11

12

また、実行器の変更先が指定されると、記録媒体に格納された第1の固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【0019】請求項2に係る発明においては、ソフトウェアを実行する実行器の変更先が指定されたとき、記録媒体に格納された累積数および実行不可情報記憶手段に記憶された基準数のそれぞれに所定値を加算するようにしている。その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、累積数が基準数よりも大きい場合のみ、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。これによって、変更先の実行器において再び元の実行器が変更先として指定された場合、元の実行器でのソフトウェアの実行が可能となる。

【0020】請求項3に係る発明においては、ソフトウェアを実行する実行器の変更先が指定されたとき、実行器で乱数を発生し、この乱数を実行不可情報記憶手段に追加して書き込むと共に、記録媒体に格納された乱数を当該乱数で書き換えるようにしている。その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。これによって、変更先の実行器において再び元の実行器が変更先として指定された場合、元の実行器でのソフトウェアの実行が可能となる。

【0021】請求項4に係る発明においては、暗号化されたソフト鍵を記録媒体に格納しておき、実行器では、このソフト鍵を固有の秘密情報を用いて復号化し、さらに復号化されたソフト鍵を用いて、記録媒体から読み出したソフトウェアを復号化し実行するようにしている。これによって、ソフトウェアを実行可能な実行器を予め特定することができる。また、ソフトウェアを実行する実行器の変更先が指定されると、復号化されたソフト鍵を、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納された暗号化されたソフト鍵を、このとき暗号化されたソフト鍵に書き換えるようにしている。これによって、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている

ソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【0022】請求項5に係る発明においては、暗号化されたソフトウェア、ソフトウェア固有情報、暗号化されたソフト鍵および累積数の内、少なくともいずれか1つを対象として作成されたデジタル署名情報を記録媒体に格納しておき、実行器では、記録媒体に格納されているデジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、記録媒体の格納情報の正当性をより正確に確認でき、不正な複製品を防止できる。

【0023】請求項6に係る発明においては、記録媒体がコピーされる毎に更新される累計数を実行器に記憶しておき、記録媒体に格納されたコピー可能回数が当該累計数よりも大きい場合のみ、当該記録媒体のコピーを許可するようにしている。これによって、記録媒体のコピー回数を予め定められた回数に制限することができる。

【0024】請求項7に係る発明においては、貸し主側の実行器は、記録媒体に格納された第1のソフト鍵を用いてソフトウェアの復号化を行う。したがって、借り主側の実行器では、記録媒体を貸し主に返却するとき、記録媒体中の第2のソフト鍵を書き換える必要がない。

【0025】請求項8に係る発明においては、記録媒体に格納されたソフトウェア自体が、指定された実行器でのみ復号可能なように暗号化されている。したがって、実行器では、固有の秘密情報を用いて、ソフトウェアを復号化し実行する。

【0026】

【実施例】

(1) 第1の実施例

図1は、本発明の第1の実施例に係るソフトウェア保護システムの構成を示すブロック図である。なお、図1において、実線の矢印はデータの移動を示し、破線の矢印は制御情報の移動を示している。また、以下の説明において、ソフトウェアとは、例えばアプリケーションプログラムを意味するものとする。

【0027】図1において、ディスク1は、暗号化ソフトウェア記録部11と、情報記録部12を含む。暗号化ソフトウェア記録部11には、暗号化ソフトウェアE(KA, software)が格納されている。情報記録部12には、ソフトウェアの種別を表すソフトウェア固有情報IDAおよびソフトウェアを実行できる指定実行器の変更回数を表す累積数CNT[A]を含むソフトウェア識別子と、指定された実行器でしか復号できない指定実行器用ソフト鍵E(X, KA)と、これら各情報の正当

(8)

特開平7-244584

13

性を示す署名情報とが記録されている。

【0028】プレーヤ2は、ディスク1内のソフトウェア識別子、指定実行器用ソフト鍵E(X, KA)および署名情報の内容を確認してソフトウェアの実行を行ない、さらに指定実行器の変更手続きを行なう機能を有している。このプレーヤ2は、接続部201と、ソフトウェアID検索部202と、記憶部203と、署名情報確認部204と、実行制御部205と、基準数・累積数比較部206と、ソフト鍵暗号化／復号化部207と、秘密情報格納部208と、暗号化ソフトウェア復号部209と、ソフトウェア実行部210と、実行器指定部211と、実行不可ソフトウェア情報更新部212と、署名情報作成部213とを備えている。

【0029】接続部201は、ディスク1をプレーヤ2に着脱自在に接続するもので、ディスク1から各情報を読み出し、ディスク1に所定の情報を書き込む機能を有している。ソフトウェアID検索部202は、入力されるソフトウェア固有情報IDAが、記憶部203に実行不可ソフトウェアとして記憶されているかどうかを検索する機能を有している。記憶部203は、実行不可ソフトウェアのソフトウェア固有情報IDA'と、ソフトウェアを実行不可状態にしたときの情報記録部12に記録されている累積数CNT[A]と同じ値である基準数NUM[A]を対にしてソフトウェア識別子として記憶している。

【0030】署名情報確認部204は、記憶部203において実行不可ソフトウェアとして記録されているソフトウェアに対して、情報記録部12に記録されている署名情報が正当なものかどうかを確認し、署名情報が正当な場合は基準数・累積数比較部206に基準数NUM[A]と累積数CNT[A]の比較を行うように指示し、署名情報が不当な場合は実行制御部205にそのソフトウェアの実行不許可の情報を入力する機能を有している。実行制御部205は、署名情報確認部204から入力される情報(情報記録部12に記録された署名情報が正当か否かを示す情報)と、基準数・累積数比較部206から入力される情報(そのソフトウェアの実行許可・不許可の情報)とに基づいて、暗号化ソフトウェアE(KA, softA)を復号化するかどうかの制御を行なう機能を有している。基準数・累積数比較部206は、署名情報確認部204で署名情報が正当と確認されたディスク1に対して、記憶部203に記憶されている該ソフトウェアの基準数NUM[A]と情報記録部12に記録されている累積数CNT[A]との大小関係を比較し、その結果に基づいてソフトウェアの実行許可・不許可の情報を実行制御部205に入力する機能を有している。

【0031】ソフト鍵暗号化／復号化部207は、情報記録部12に記録されている指定実行器用ソフト鍵E(X, KA)を、秘密情報格納部208に格納されてい

14

るプレーヤ2に固有の秘密情報SXで復号化し、また指定された実行器の変更がある場合は、変更先用の指定実行器用ソフト鍵に暗号化する機能を有している。秘密情報格納部208は、プレーヤ2に固有の秘密情報SXを記録している。暗号化ソフトウェア復号部209は、暗号化ソフトウェア記録部11に記録されている暗号化ソフトウェアE(KA, softA)が入力され、ソフト鍵暗号化／復号化部207で復号化されたソフト鍵で、暗号化ソフトウェアE(KA, softA)を復号化する機能を有している。ソフトウェア実行部210は、暗号化ソフトウェア復号部209で復号化されたソフトウェアsoftAを実行する機能を有している。

【0032】実行器指定部211は、入力された変更先情報に従って指定先実行器用ソフト鍵の変更をソフト鍵暗号化／復号化部207で行うように制御し、情報記録部12に記録されている累積数CNT[A]の書き換えを行うように接続部201に指示し、それに伴い記憶部203に記憶されている情報の変更を実行不可ソフトウェア情報更新部212に指示し、新しいソフトウェア識別子に対する署名情報の作成を署名情報作成部213に指示する機能を有している。実行不可ソフトウェア情報更新部212は、指定実行器の変更のときに、情報記録部12に記録されている累積数の書き換えを行うのに伴い、記憶部203に記憶されている情報の変更を行なう機能を有している。署名情報作成部213は、実行不可ソフトウェア情報更新部212によって変更された新しいソフトウェア識別子に対する署名情報の作成を行なう機能を有している。

【0033】なお、図1のプレーヤ2内において、ソフトウェアID検索部202、記憶部203、署名情報確認部204、実行制御部205、基準数・累積数比較部206、ソフト鍵暗号化／復号化部207、秘密情報格納部208、暗号化ソフトウェア復号部209、ソフトウェア実行部210、実行器指定部211、実行不可ソフトウェア情報更新部212および署名情報作成部213は、それぞれ変更、解析、複製できない領域に配置されている。

【0034】概説すると、上記第1の実施例のソフトウェア保護システムは、ソフトウェアsoftA自体はそのソフトウェアの全ディスク共通の鍵ソフト鍵KAで暗号化し、そのソフト鍵KAをその指定された実行器であるプレーヤ2でしか復号できないように暗号化することによって、指定された実行器以外では実行できないことを実現している。

【0035】図2は、上記第1の実施例のソフトウェア保護システムにおけるソフトウェア実行動作の処理手順を示すフローチャートである。また、図3は、上記第1の実施例のソフトウェア保護システムにおける指定実行器の変更手続きの処理手順を示すフローチャートである。以下、これら図2および図3を参照して、上記第1

50

(9)

特開平7-244584

15

の実施例の動作を説明する。

【0036】なお、以下では、図1のプレーヤ2（以下、プレーヤXと表現する）用として暗号化されたソフト鍵E（X，KA）を持つ暗号化ソフトウェアE（KA，softA）が復号化されて実行され、その後、図示しない他のプレーヤ（以下、プレーヤYと表現する）用に指定プレーヤの変更手続きを行なう場合の動作について説明する。また、以下の説明において、ソフト鍵E（X，KA）は、ソフト鍵KAをプレーヤXに固有の秘密情報SXでのみ復号化される形式で暗号化したものを示している。また、ソフトウェアE（KA，softA）は、ソフトウェアsoftAをソフト鍵KAで暗号化したものを示し、ソフト鍵KAで復号化される。

【0037】（a）暗号化ソフトウェアの復号・実行動作

最初に、図2を参照して、暗号化ソフトウェアの復号・実行動作を説明する。まず、接続部201にディスク1が接続される（ステップS101）。次に、情報記録部12に記録されているソフトウェア識別子のソフトウェア固有情報IDAが、接続部201を通してソフトウェアID検索部202に入力される。ソフトウェアID検索部202は、当該入力されたソフトウェア固有情報IDAと一致する実行不可ソフトウェア固有情報IDA'が、記憶部203に記憶されているかどうかを検索する（ステップS102）。

【0038】上記ステップS102における検索の結果、入力されたソフトウェア固有情報IDAと一致する実行不可ソフトウェア固有情報IDA'が記憶部203に記憶されている場合、ソフトウェアID検索部202は、接続部201を介して、情報記録部12から署名情報とソフトウェア識別子とを読み出し、署名情報確認部204に入力する。署名情報確認部204は、情報記録部12に記録されているソフトウェア識別子の内容が正当なものであるかどうかを、署名情報のデジタル署名作成者の実行器識別子（図示していないが、ディスク1内に格納されている）から容易に導かれるデジタル署名作成者の公開鍵で確認する（ステップS103）。ステップS103での確認の結果、ソフトウェア識別子が正当なものでないと判断した場合、署名情報確認部204は、実行制御部205にそのソフトウェアの実行を不許可とするように指示する（ステップS104）。従って、実行制御部205は、ソフトウェアの実行を行わない。

【0039】一方、上記ステップS103における確認の結果、ソフトウェア識別子の内容が正当なものであると判断した場合、署名情報確認部204は、基準数・累積数比較部206に対して、記憶部203にソフトウェア識別子として実行不可ソフトウェア固有情報IDA'と対に記憶されている基準数NUM[A]を、情報記録部12内に記録されているソフトウェア識別子の累積数

16

CNT[A]と比較するように指示する。応じて、基準数・累積数比較部206は、記憶部203からソフトウェア識別子として実行不可ソフトウェア固有情報IDA'と対で記録されている基準数NUM[A]を読み出す。また、接続部201を介して、情報記録部12に記録されているソフトウェア識別子の累積数CNT[A]を読み出す。次に、基準数・累積数比較部206は、入力された基準数NUM[A]と累積数CNT[A]とを比較する（ステップS105）。

【0040】ディスク1に格納されたソフトウェアが正当なソフトウェアである場合は、後述の指定プレーヤ変更手続きにより、不等式NUM[A]<CNT[A]が成り立ち、基準数・累積数比較部206は、実行制御部205にソフトウェアの実行許可情報を入力する（ステップS106）。一方、不等式NUM[A]<CNT[A]が成り立たない場合は、ディスク1は指定実行器変更手続きによりすでに無効になったディスクであるので、実行制御部205にそのソフトウェアsoftAの実行不許可の情報を入力する（ステップS104）。したがって、この場合、実行制御部205は、ソフトウェアsoftAの実行を行わない。

【0041】基準数・累積数比較部206からソフトウェアの実行許可が出た場合、実行制御部205は、接続部201を介して、情報記録部12から指定実行器用ソフト鍵E（X，KA）を読み出し、ソフト鍵暗号化／復号化部207に入力する。また、実行制御部205は、秘密情報格納部208からプレーヤXに固有の秘密情報SXを読み出して、ソフト鍵暗号化／復号化部207に入力する。応じて、ソフト鍵暗号化／復号化部207は、指定実行器用ソフト鍵E（X，KA）をプレーヤXに固有の秘密情報SXで復号化し、ソフト鍵KAを得る（ステップS107）。なお、このとき、指定プレーヤ用ソフト鍵E（X，KA）がプレーヤX用でないならば、ソフト鍵KAが復号できずソフトウェアは実行できない。

【0042】次に、ソフト鍵暗号化／復号化部207は、復号化されたソフト鍵KAを、暗号化ソフトウェア復号部209に入力する。また、実行制御部205は、接続部201を介して、ディスクの暗号化ソフトウェア記録部8から暗号化ソフトウェアE（KA，softA）を読み出し、暗号化ソフトウェア復号部209に入力する。応じて、暗号化ソフトウェア復号部209は、ソフト鍵暗号化／復号化部207から入力されたソフト鍵KAを用いて、ソフトウェアsoftAを復号化する（ステップS108）。次に、暗号化ソフトウェア復号部209は、その復号化されたソフトウェアsoftAをソフトウェア実行部210に入力する。従って、ソフトウェア実行部210は、復号化されたソフトウェアを実行する（ステップS109）。

【0043】一方、前述のステップS102における検

50

(10)

特開平7-244584

17

索の結果、入力されたソフトウェア固有情報IDAと一致する実行不可ソフトウェア固有情報IDA'が記憶部203に記憶されていない場合、ソフトウェアID検索部202は、実行制御部205にソフト実行許可の情報を入力する(ステップS106)。以下、ステップS107~S109の処理は、前述のステップS107~S109の動作と全く同じである。

【0044】(b) 指定実行器の変更手続き

次に、図3を参照して、指定実行器の変更手続きについて説明する。なお、以下の説明では、現在プレーヤXでしか実行できないディスク1に格納されているソフトウェアをプレーヤXでは実行不可とし、プレーヤXと異なる他のプレーヤYで実行できるようにする指定実行器変更手続きについて述べる。

【0045】まず、変更先をプレーヤYにするという情報(実行器識別子)が、図示しないキーボード、マウス等の入力装置から実行器指定部211に入力される(ステップS201)。すると、実行器指定部211は、接続部201を介して、情報記録部12から指定実行器用ソフト鍵E(X, KA)を読み出し、ソフト鍵暗号化/復号化部207に inputsする。また、実行器指定部211は、秘密情報格納部208からプレーヤXに固有の秘密情報SXを読み出し、ソフト鍵暗号化/復号化部207に inputsする。ソフト鍵暗号化/復号化部207は、秘密情報格納部208から入力されるプレーヤXに固有の秘密情報SXを用いて、指定実行器用ソフト鍵E(X, KA)をソフト鍵KAに復号化し、その後、実行器指定部211から与えられる変更先プレーヤYの実行器識別子からプレーヤY用の公開鍵を生成し、この生成した公開鍵を用いてソフト鍵KAを暗号化し、プレーヤY用ソフト鍵E(Y, KA)を得る(ステップS202)。また、実行器指定部211は、先に情報記録部12に記録されているプレーヤX用ソフト鍵E(X, KA)を、接続部201を介して消去する。さらに、実行器指定部211は、接続部201を介して、情報記録部12に、プレーヤY用ソフト鍵E(Y, KA)を指定実行器用ソフト鍵として記録する。このプレーヤY用ソフト鍵E(Y, KA)は、プレーヤYに固有の秘密情報SY(プレーヤYの秘密情報部208に格納されている)のみによってしか復号化できない。したがって、以後このディスク1は、プレーヤYでしか実行できなくなる。

【0046】次に、実行器指定部211は、接続部201を介して、情報記録部12に記録されているソフトウェア識別子の累積数CNT[A]の値が1だけ増えるように記録を更新する(ステップS203)。次に、実行器指定部211は、更新された新しい累積数CNT[A]の値を新しいソフトウェア識別子の基準数NUM[A]の値とし、実行不可ソフトウェア固有情報IDA'と対にしてソフトウェア識別子として、実行不可ソフトウェア情報更新部212を介して、記憶部203に

18

書き込む(ステップS204)。このとき、実行器指定部211は、同時に記憶部203から古い基準数の値を消去する。これによって、このディスク1に格納されているソフトウェアは、以後、プレーヤXでは実行できなくなる。

【0047】次に、実行器指定部211は、接続部201を介して、情報記録部12からソフトウェア識別子であるソフトウェア固有情報IDAと累積数CNT[A]とを読み出し、また秘密情報格納部208からプレーヤXに固有の秘密情報SXを読み出し、それぞれ署名情報作成部213に inputsする。署名情報作成部213は、入力されたソフトウェア識別子であるソフトウェア固有情報IDAと累積数CNT[A]に対して、プレーヤXに固有の秘密情報SXを用いてプレーヤXでしか作成できない署名情報を作成し、この作成された署名情報を接続部201を介して新たな署名情報として情報記録部12に記録する(ステップS205)。このとき、署名情報作成部213は、同時に古い署名情報を消去する。

【0048】なお、上記指定プレーヤ変更手続き前にプレーヤX用のディスクをコピーしておいても、指定プレーヤ変更手続き後には、記憶部203での基準数NUM[A]が、このコピーされたディスクの累積数よりも大きくなるので、図2のステップS105におけるプレーヤ内の基準数NUM[A]とディスク内の累積数CNT[A]との比較動作で実行不可と判断され、プレーヤXで不所望にコピーディスクが実行されることを防止できる。

【0049】以上説明したように、第1の実施例によれば、ソフト鍵を指定実行器以外では復号できないようなソフトウェア保護システムにおいて、指定実行器の変更を可能とし、不正なコピーを防止しつつ、ソフトウェアを任意の実行器で実行できる環境を実現することができる。

【0050】なお、上記第1の実施例は、ソフトウェア本体をそのソフトウェアの全ディスクに共通のソフト鍵KAで暗号化し、そのソフト鍵KAを指定された実行器でしか復号できないように暗号化するシステムとして構成されているが、本発明は、ソフトウェア自身を指定した実行可能実行器でしか復号できないように暗号化するように構成されてもよく、この場合も第1の実施例と同様な効果が得られる。

【0051】また、上記第1の実施例では、ソフトウェアを指定実行器以外で実行されないようにするためにソフト鍵を用いたが、ディスクに指定実行器のID情報を格納しておき、実行器側ではいつもソフトウェアの実行を行う前に、ディスクのID情報が自装置に対応するID情報かをチェックし、自装置に対応するID情報の場合のみソフトウェアを実行するようにしてもよい。

【0052】また、上記第1の実施例では、ディスク1を譲渡する際に、無効ディスクを示す情報として、順序

10

20

30

40

50

(11)

19

付けられた数を有する累積数および基準数を用いたが、これら累積数および基準数に代えて乱数を発生し、情報記録部12および記憶部203には、この乱数をソフトウェア固有情報と対にしてソフトウェア識別子として記録しておくようにしてもよい。この場合、記憶部203には発生した乱数が全て消去せずに記録され、情報記録部12には新しい乱数が発生する毎に古い乱数が新しい乱数に書き換えられる。そして、ディスク1上のソフトウェア識別子を記憶部203に記憶されている全てのソフトウェア識別子と比較し、一致するものがない場合にのみソフトウェアの実行を許可することになる。

【0053】また、上記第1の実施例では、ディスク1上のソフトウェア識別子の正当性を確保するため、これを対象としたデジタル署名を生成したが、デジタル署名の対象をソフトウェア識別子と指定実行器用ソフト鍵と暗号化ソフトウェアの内容の全部または一部を対象としてもよい。これによって、暗号化ソフトウェア記録部11に記録されている暗号化ソフトウェアの内容および実行器識別子の正当性も確保することができる。

【0054】また、上記第1の実施例では、ディスク1上のデータの正当性を示すためにデジタル署名を使用しているが、ソフトウェア識別子などを指定実行器以外では復号できない形で暗号化してもよく、この場合も上記第1の実施例と同様な効果が得られる。

【0055】また、上記第1の実施例では、ソフトウェア識別子のソフトウェアを識別する情報として、ソフトウェア種別毎に異なり、かつディスク毎には共通のソフトウェア固有情報IDAを用いたが、これに代えて各ディスクに固有の識別子を用いてもよい。これによって、ディスク1の指定実行器変更手続き後に、先のディスクと同じ種別のソフトウェアを格納する別のディスクを実行しようとするときにも対処できる。

【0056】また、上記第1の実施例では、オフラインのソフトウェア流通形態を想定しているが、この発明をオンラインのソフトウェア流通形態に適用しても、上記第1の実施例と同様な効果が得られる。

【0057】(2) 第2の実施例

本発明の第2の実施例は、第1の実施例で述べたソフトウェア保護システムを用いたレンタルソフトウェアシステムとして構成されている。図4は、この第2の実施例のレンタルソフトウェアシステムにおける処理手順を示すフローチャートである。以下、第1の実施例で述べた構成を援用しつつ、図4を参照して、第2の実施例の詳細を説明する。

【0058】このレンタルソフトシステムでは、レンタル専用のディスクを導入する。第1の実施例では、ディスク1の情報記録部12（図1参照）には、ソフト鍵に関する情報として、暗号化された指定実行器用ソフト鍵のみが記録されている。これに対し、第2の実施例におけるレンタル専用ディスクでは、ディスク内の情報記録

特開平7-244584

20

部12に、指定実行器用ソフト鍵だけではなく、レンタル店用ソフト鍵が常に記録されている。情報記録部12におけるその他の情報は、第1の実施例において情報記録部12に記録されている情報と同じである。

【0059】レンタル店Xで会員Y（プレーヤYと同じものとする）に、上記レンタル専用ディスクを貸す場合の手続きを述べる。レンタル店Xでは、会員Yを変更先として第1の実施例で述べたように変更手続きをレンタル店のプレーヤで行なう。このとき、このディスク1内の指定実行器用ソフト鍵が、会員YのプレーヤYでしか実行できない形式に暗号化されている（ステップS301）。会員Yは、自分自身のプレーヤYに、このディスク1を差し込み、ソフトウェアを実行させる（ステップS302）。以下、このディスク1内のソフトウェアが実行される手順は、第1の実施例で述べた通りである。

【0060】次に、会員Yがディスクをレンタル店Xに返却する場合について述べる。会員Yは、第1の実施例で述べた指定実行器変更手続きで、譲渡先としてレンタル店を指定するのではなく、単に返却手続きをすればよい。なぜならば、ディスク1の情報記録部12には、常にレンタル店用ソフト鍵が記録されているため、レンタル店Xでは、このレンタル店用ソフト鍵を用いて、ディスク1の実行が可能であるためである。このとき、会員Yのプレーヤにおける実行器指定部211は、情報記録部12のプレーヤY用ソフト鍵を消去し、累積数を1増やし、記憶部203の基準数の更新を行なう（ステップS303）。この処理によって、レンタル用ディスクをコピーしてにおいて返却手続き後に実行しようとしても、図2のステップS105によってそのコピーディスクは実行できない。すなわち、レンタル専用ディスクでは、会員Y用のソフト鍵の消去はできるが、指定実行器の変更手続きは、レンタル店でのみ可能である。

【0061】上記のように第2の実施例によれば、レンタル先用に暗号化されたレンタルソフトウェアをレンタル店に返却するときに、会員側ではレンタル店を指定実行器として指定実行器の変更手続きを行う必要がなく、面倒な手間が省ける。また、レンタル専用ディスクは指定実行器でしか実行できないため、レンタルソフトウェアのまた貸しも防げる。さらに、累積数と基準数との更新により、会員が不正なコピーを作成するのにも防げる。また、レンタル専用ディスクの指定実行器の変更手続きが可能なのはレンタル店のみであるから、会員間の貸し借りもできない。

【0062】(3) 第3の実施例

図5は、本発明の第3の実施例の構成を示すブロック図である。図5において、この第3の実施例では、指定された回数だけコピーができるマスターディスク10を用いる。このマスターディスク10には、図1のディスク1に記録されている情報に加えて、コピー可能回数N o

50

(12)

特開平7-244584

21

【copy】、累計数SUM[disk]およびマスターディスク識別子が情報記録部12に記録されている。マスターディスク10のその他の記録情報は、図1のディスク1の記録情報と同様である。

【0063】プレーヤ2には、第1の実施例で述べたプレーヤ2の構成に加えて、コピー制御部214およびバッファメモリ215が追加されている。図6は、この第3の実施例のソフトウェア保護システムにおける処理手順を示すフローチャートである。以下、この図6を参照して、第3の実施例の動作を説明する。

【0064】まず、マスターディスク10からコピーディスクを作成する場合について説明する。なお、マスターディスク10は、プレーヤXでのみ実行できるものとする。マスターディスク10が接続部201に接続されると(ステップS401)、コピー制御部214は、情報記録部12からマスターディスク識別子を読み出し、接続されたディスクがマスターディスク10であることを識別する(ステップS402)。次に、コピー制御部214は、情報記録部12から累計数SUM[disk]を読み出し、マスターディスク10からのコピーが最初か否かを判断する(ステップS403)。マスターディスク10から1度もコピーディスクが作成されていない場合(すなわち、累計数SUM[disk]が0の場合)、コピー制御部214は、実行不可ソフトウェア情報更新部212は、接続部201を介して、情報記録部12からコピー可能回数No[copy]および累計数SUM[disk]を読み出し、記憶部203に、それぞれ、No[copy, X]およびSUM[X]として格納する(ステップS404)。また、コピー制御部214は、接続部201を介して、情報記録部12からマスターディスク識別子を読み出し、上記コピー可能回数No[copy, X]および累計数SUM[X]と対にして、記憶部203に格納する。

【0065】一方、マスターディスク10から少なくとも1度はコピーディスクが作成されている場合、コピー制御部214は、記憶部203に記憶されているコピー可能回数No[copy, X]および累計数SUM[X]と、情報記録部12に記録されているコピー可能回数No[copy]および累計数SUM[disk]とを比較し、両者が等しいか否かを確認する(ステップS405)。ステップS405において両者の不一致が確認された場合、コピー制御部214は、マスターディスク10からのコピーが不許可であると判断する(ステップS406)。したがって、この場合、マスターディスク10のコピーは行われぬ。一方、ステップS405において両者の一致が確認された場合、コピー制御部214は、情報記録部12に記録されたコピー可能回数No[copy]と、記憶部203に記憶された累計数SUM[X]との大小関係と比較し、不等式No[copy] > SUM[X]が成り立つ場合にのみ、マスター

22

ディスク10からのコピーを許可する(ステップS407)。

【0066】次に、マスターディスク10のコピー許可が出て、別のディスクにマスターディスクの内容をコピーする場合の動作について説明する。連続して1度にコピーをする回数nが、外部の入力装置(図示せず)からコピー制御部214に対して入力されると、コピー制御部214は、接続部201を介して、情報記録部12に記録されている累計数SUM[disk]を指定されたコピー回数nだけ増加するように更新し、同様に、記憶部203内の累計数SUM[X]を更新する(ステップS408)。ただし、このnは、更新される累計数が、コピー可能回数No[copy]と等しくまたは大きくなならないような値に選ばれる。次に、コピー制御部214は、接続部201を介して、マスターディスク10から暗号化ソフトウェアおよび指定実行器用ソフト鍵を読み出し、バッファメモリ214に格納する(ステップS409)。

【0067】コピーディスクは、第1の実施例で述べたディスクと同じ記録形式で、情報記録部12と暗号化ソフトウェア記録部8とを含む。このコピーディスクがマスターディスク10と差し替えられて接続部201に接続されると(ステップS410)、図示しない外部の入力装置から実行器指定部211に、指定実行器に関する情報が入力される(ステップS411)。この実行器指定情報は、コピー制御部211に入力される。応じて、コピー制御部214は、バッファメモリ215から暗号化ソフトウェアを読み出し、接続部201を介して、コピーディスクの暗号化ソフトウェア記録部11に書き込む(ステップS412)。また、コピー制御部214は、コピーディスクの情報記録部12に、ソフトウェア識別子として、ソフトウェア固有情報と累積数を記録する(ステップS412)。このとき、累積数は0で記録される。さらに、コピー制御部214は、指定実行器用ソフト鍵および署名情報を、それぞれ、ソフト鍵暗号化/復号化部207および証明情報作成部213によって作成させ、接続部201を介してコピーディスクの情報記録部12に記録させる(ステップS412)。これで、新しいコピーディスクが1つ生成されたことになる。その後、コピー制御部214は、予め指定されたコピー回数nだけのコピーディスクを生成する。n個のコピーディスクが生成されると、コピー制御部214は、バッファメモリ215に格納されている暗号化ソフトウェアを消去する(ステップS413)。

【0068】以上のように、上記第3の実施例によれば、新たにある指定された特定の実行器でしか実行できないコピーディスクを、予め指定された回数だけ生成することができる。

【0069】

【発明の効果】請求項1の発明によれば、ソフトウェア

10

20

30

40

50

(13)

特開平7-244584

23

を実行させるべき実行器に固有の第2の固有情報を記録媒体に格納しておき、実行器では、記録媒体からソフトウェアおよび第2の固有情報を読み出し、当該第2の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるようにしている。指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定されると、記録媒体に格納された第2の固有情報を、指定された他の実行器に固有の情報に変換するようにしている。ソフトウェアを実行可能な実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納された第1の固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けられないようにしている。実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【0070】請求項2の発明によれば、実行器の変更先が指定されたとき、記録媒体に格納された累積数および実行不可情報記憶手段に記憶された基準数のそれぞれに所定値を加算しておき、その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、累積数が基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。そのため、変更先の実行器において再び元の実行器が変更先として指定された場合であっても、元の実行器でのソフトウェアの実行が可能となる。

【0071】請求項3の発明によれば、実行器の変更先が指定されたとき、実行器で乱数を発生し、この乱数を実行不可情報記憶手段に追加して書き込むと共に、記録媒体に格納された乱数を当該乱数で書き換え、その後、実行不可情報記憶手段に記憶されている第1の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。そのため、変更先の実行器において再び元の実行器が変更先として指定された場合であっても、元の実行器でのソフトウェアの実行が可能となる。

【0072】請求項4の発明によれば、暗号化されたソフト鍵を記録媒体に格納しておき、実行器では、このソフト鍵を固有の秘密情報を用いて復号化し、さらに復号化されたソフト鍵を用いて、記録媒体から読み出したソフトウェアを復号化し実行するようにしている。指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定され

24

ると、復号化されたソフト鍵を、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納された暗号化されたソフト鍵を、このとき暗号化されたソフト鍵に書き換えるようにしている。ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されているソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けられないようにしている。実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【0073】請求項5の発明によれば、暗号化されたソフトウェア、ソフトウェア固有情報、暗号化されたソフト鍵および累積数の内、少なくともいずれか1つを対象として作成されたデジタル署名情報を記録媒体に格納しておき、実行器では、記録媒体に格納されているデジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けられないようにしている。記録媒体の格納情報の正当性をより正確に確認でき、不正な複製品を防止できる。

【0074】請求項6の発明によれば、記録媒体がコピーされる毎に更新される累計数を実行器に記憶しておき、記録媒体に格納されたコピー可能回数が当該累計数よりも大きい場合のみ、当該記録媒体のコピーを許可するようにしている。記録媒体のコピー回数を予め定められた回数に制限することができる。

【0075】請求項7の発明によれば、貸し主側の実行器は、記録媒体に格納された第1のソフト鍵を用いてソフトウェアの復号化を行うので、借り主側の実行器では、記録媒体を貸し主に返却するとき、記録媒体中の第2のソフト鍵を書き換える必要がない。

【0076】請求項8の発明によれば、記録媒体に格納されたソフトウェア自体が指定実行器でのみ復号可能なように暗号化されているので、指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定されると、復号化されたソフトウェアを、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納されたソフトウェアを、このとき暗号化されたソフトウェアに書き換えるようにしている。ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されているソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒

50

(14)

特開平7-244584

25

26

体に格納されているソフトウェアの実行を受け付けられないようにしているので、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止できる。

【図面の簡単な説明】

【図1】本発明の第1の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図2】本発明の第1の実施例のソフトウェア保護システムにおけるソフトウェア実行動作の処理手順を示すフローチャートである。

【図3】本発明の第1の実施例のソフトウェア保護システムにおける指定実行器の変更手続きの処理手順を示すフローチャートである。

【図4】本発明の第2の実施例のレンタルソフトウェアシステムにおける処理手順を示すフローチャートである。

【図5】本発明の第3の実施例の構成を示すブロック図である。

【図6】本発明の第3の実施例のソフトウェア保護システムにおける処理手順を示すフローチャートである。

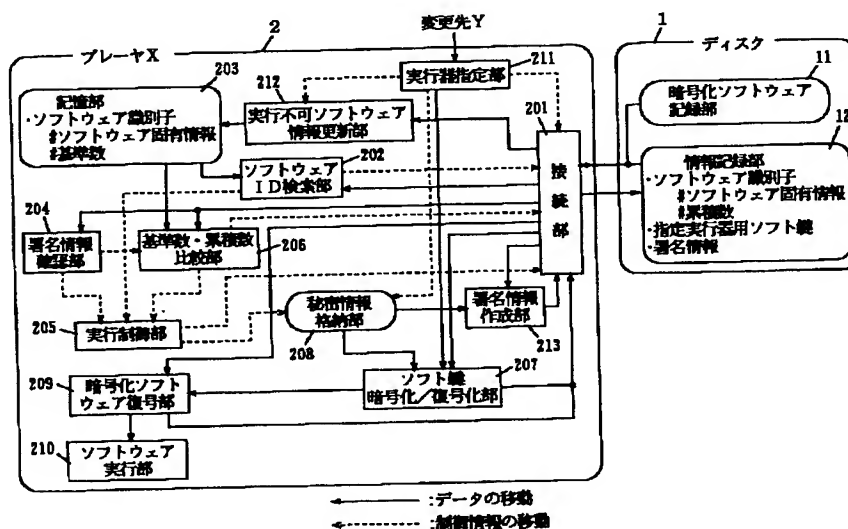
【図7】従来のソフトウェア保護システムの構成を示す*

*ブロック図である。

【符号の説明】

- 1…ディスク
- 11…暗号化ソフトウェア記録部
- 12…情報記録部
- 2…プレーヤ
- 201…接続部
- 202…ソフトウェアID検索部
- 203…記憶部
- 204…署名情報確認部
- 205…実行制御部
- 206…基準数・累積数比較部
- 207…ソフト鍵暗号化/復号化部
- 208…秘密情報格納部
- 209…暗号化ソフトウェア復号部
- 210…ソフトウェア実行部
- 211…実行器指定部
- 212…実行不可ソフトウェア情報更新部
- 213…署名情報作成部
- 214…コピー制御部

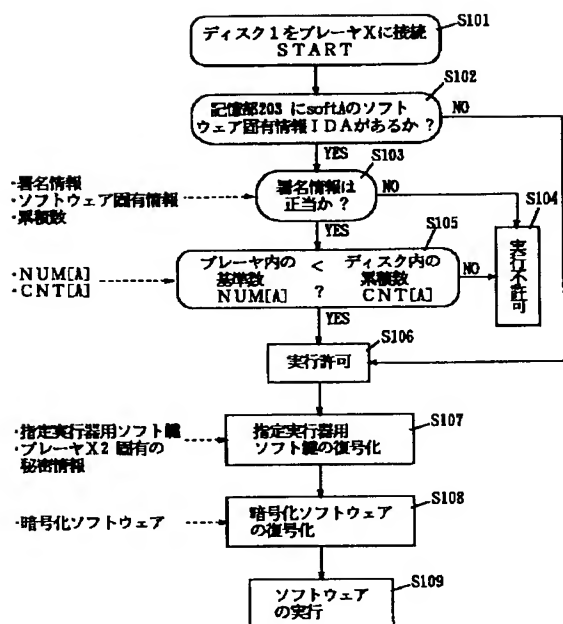
【図1】



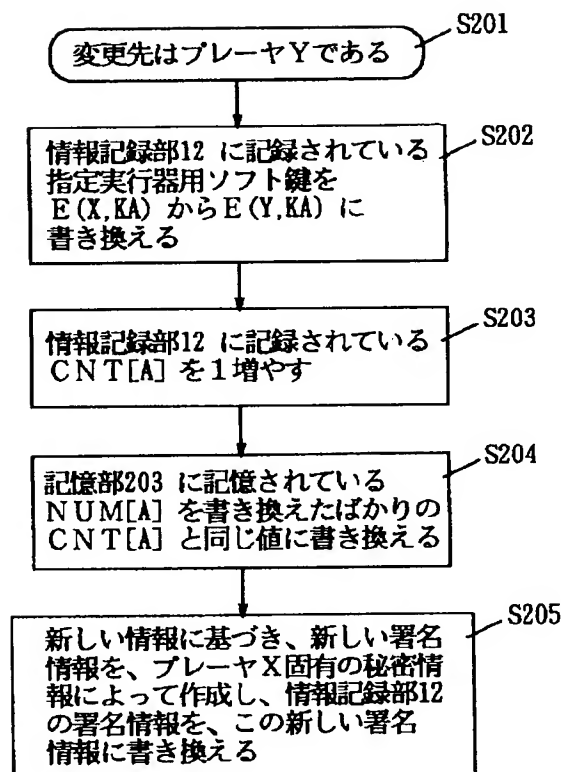
(15)

特開平7-244584

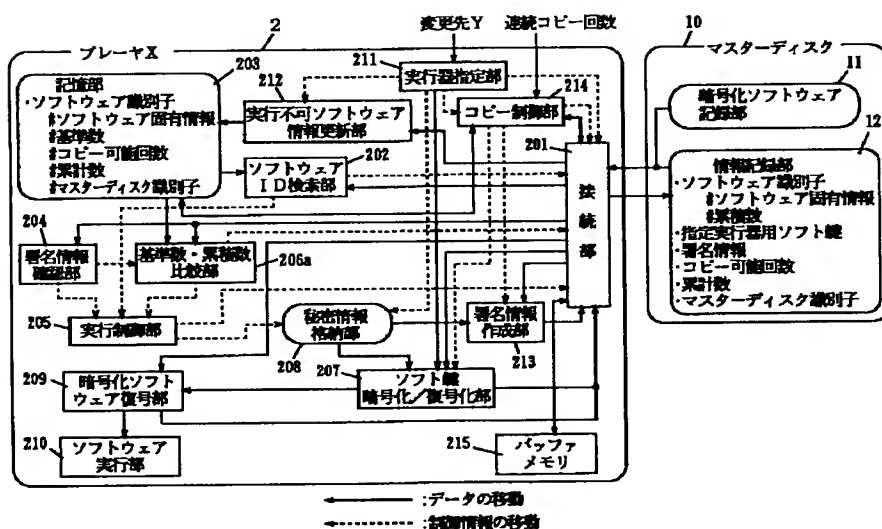
【図2】



【図3】



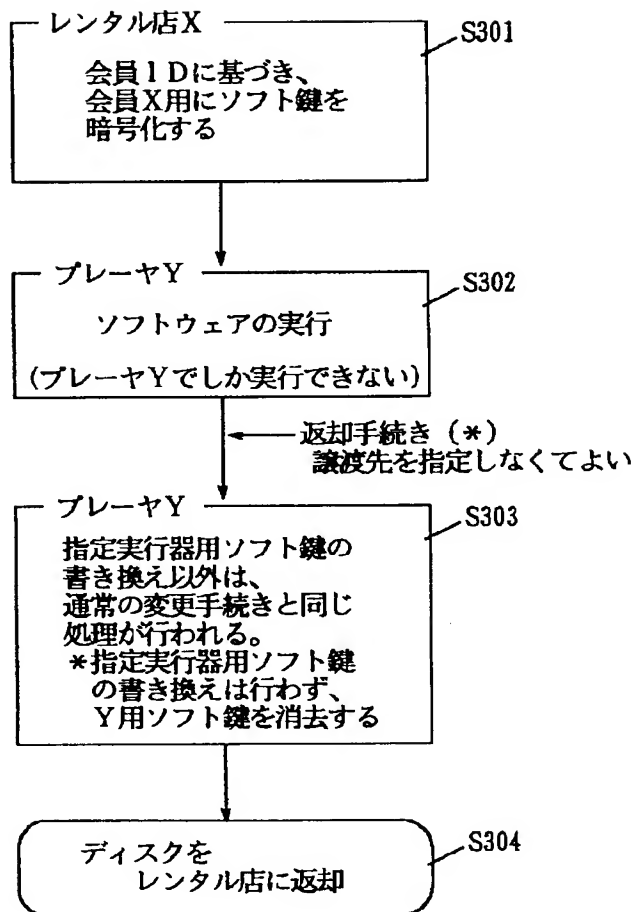
【図5】



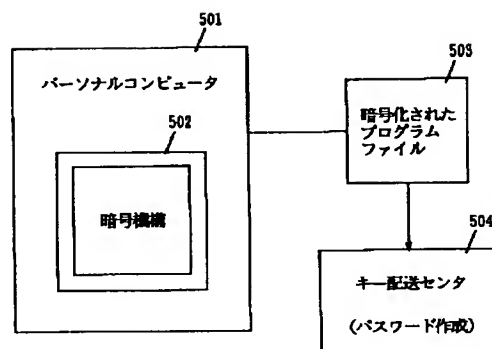
(16)

特開平7-244584

【図4】



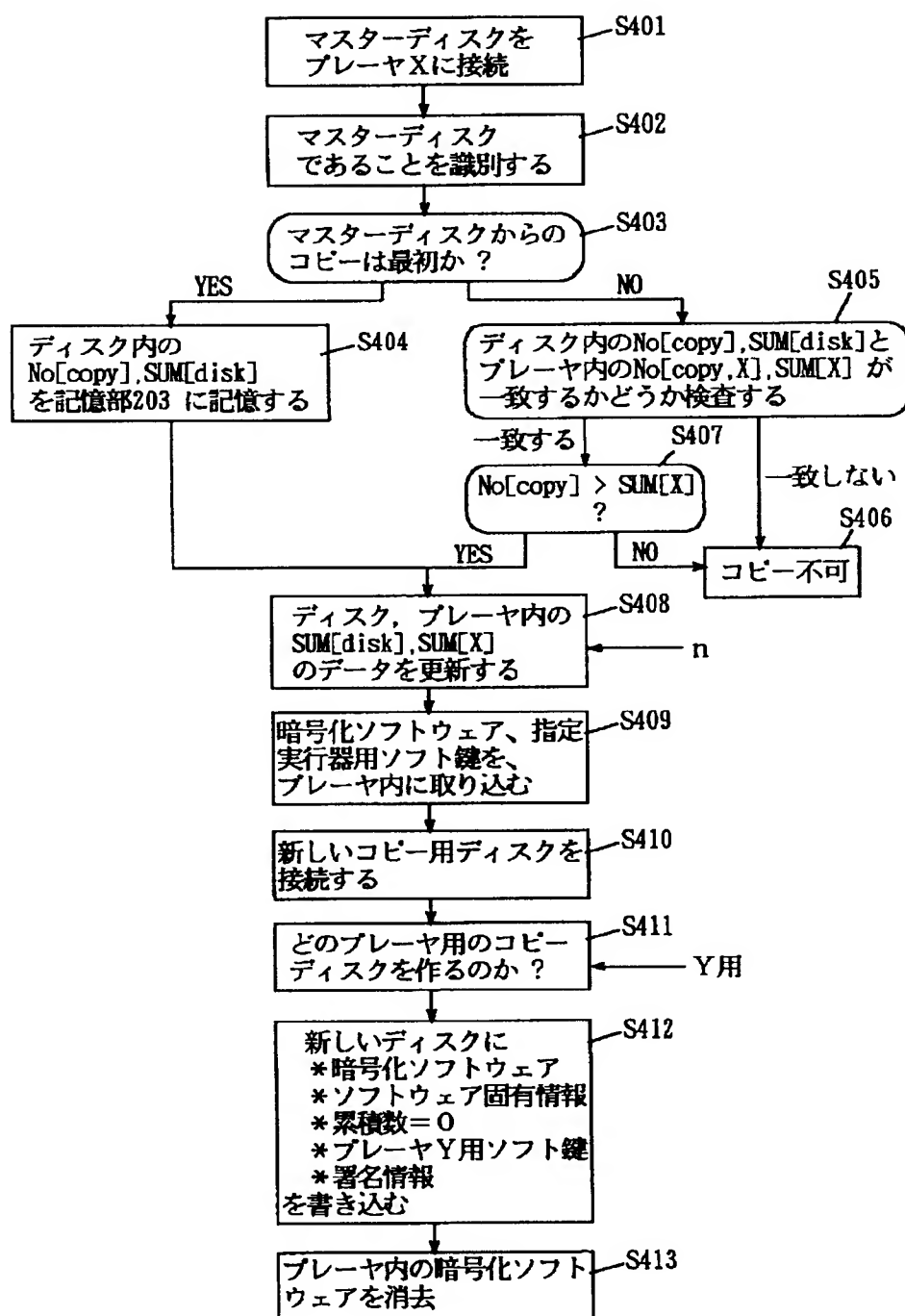
【図7】



(17)

特開平7-244584

【図6】



(18)

特開平7-244584

フロントページの続き

(72)発明者 宮地 充子
大阪府門真市大字門真1006番地 松下電器
産業株式会社内